۱۔مین-اِن-مڈل /Man-In-Middle

اس کے تفصیل میں ہم نہیں جائینگے بس اتنا سمجھ لیں کہ اس کا حملہ اس وقت ہوتا ہے جب آپ پبلک وائی فائی) یعنی وہ وائی فائی جس میں بہت سے لوگ کنیکٹ ہوں(یا نیٹ کیفے، یا جب بہت سے کمپیوٹر لین /LAN پہ کنیکٹ ہوں، یا انٹرنیٹ کا کنیکشن ایک سے زائد لوگ استعمال کر رہے ہوں، ان جگہوں پہ انٹرنیٹ استعمال کرنے سے یہ حملہ ہوسکتا ہے اور حملہ آور بھی ان میں سے ایک ہوتا ہے جو وہی انٹرنیٹ استعمال کر رہا ہو ۔ اس میں وہ آپ کے ہر ہر ویبسائٹ کی نگرانی کر سکتا ہے، اپنے فیک فیشینگ ویب سائٹ پر لے جاسکتا ہے اگر چہ آپ کوئی اور ویب سائٹ انٹر کریں پھربھی وہ اس کو ری ڈائرکٹ کر کے اپنے فیک ویب سائٹ پر لے جا سکتا ہے،اور وہ یہ بھی کر سکتا ہے کہ آپ جب بھی فیس بک کا سائٹ کھولیں تو وہ آپ کو اپنے فیک فیس بک سائٹ پہ لے جائے اور جب آپ جی میل کا سائٹ کھولیں تو وہ اپنے فیک جی میل سائٹ پہ لے جائے، اس طرح سے وہ آپ کے اکاونٹ ہیک کرسکتا ہے۔ اگر کوئی ایکسپرٹ ہو ہیکنگ میں تو وہ آپ کے کمپیوٹر کے ڈیٹا تک رسائی حاصل کر سکتا ہے۔

اس سے بچنے کا کوئی موثر طریقہ نہیں ہے ، بس یہ ہے کہ انٹرنیٹ کیفے میں تو کبھی بھی ایسا اکاونٹ نہ کھولیں، اور معلومات شئیر نہ کریں، پبلک وائی فائی میں اگر صرف خاندان کے لوگ ہیں تو کوئی مسئلہ نہیں اگر ویسے عام وائی فائی ہے تو اس سے بھی احتیاط کریں اور ایسے باقی دیگر جگہوں میں دیکھیں جہاں اطمینان ہو اسے استعمال کریں باقیوں کو استعمال نہ کریں۔

۲۔ بروٹ فورس/Brute Force

یہ سافٹوئیر میں بھی آتے ہیں اور کوڈنگ یعنی پروگرامنگ سے بھی کرتے ہیں، اس میں ہوتا یہ ہے کہ حملہ آور آپ کا اکاونٹ کھولنے کیلئے ایک لمبی تعداد میں نہ ختم ہونے والی ایک پاسورڈ کی لسٹ آزما لیگا کہ اس میں سے کوئی نہ کوئی لگ جائے ۔اس کی دو قسم ہیں:

پہلا طریقہ یہ ہے کہ اس میں سافٹوئیر خود ہی اس پاسورڈ کو ڈھونڈیگا اور aa سے شروع کریگا اس طرح پھر abپھر ac اور اسی طرح چلتا چلا جائیگا، اور اس میں پاسورڈ دھونڈنے میں گھنٹوں لگ

جاتے ہیں اور اگ پاسورڈ بہت لمبا ہو اور اس میں #$%^&* اس طرح کے نشانات ہوں تو اس کیلئے تو ایک پورا دن بھی لگ جاتا ہے اور حملہ کرنے والا مایوس ہوکر چھوڑ ہی دیتا ہے۔

دوسرا طریقہ یہ ہے کہ اس سافٹوئیر میں ایک پاسورڈ کی لسٹ ڈالتے ہیں جس میں ۱۰ ہزار سے اوپر پاسورڈ ہوتے ہیں، وہ سافٹوئیر صرف انہی پاسورڈ کو آزمائیگا، یہ پاسورڈ کی لسٹ تو نیٹ پر دستیاب ہیں وہاں سے لوگ لیتے ہیں، مگر چونکہ وہ باہر ممالک کے ہیکرز نے بنائے ہیں اور ہمارے ملک میں لوگ دوسرے پاسورڈ ڈالتے ہیں مثلاً maleer12345، karachi123، وغیرہ ، یا کسی کا نام لکھ دیتے ہیں یا کسی کا نمبر لکھ دیتے ہیں اس لئے یہ لسٹ یہاں زیادہ کارآمد نہیں ہوتی البتہ یہاں پھر حملہ کرنے والا اسی مطابق کوئی لسٹ بنائیگا یعنی لوکل لوگ جو پاسورڈ استعمال کرتے ہیں اس حساب سے بناتا ہے۔

بروٹ فورس سے بچنے کیلئے تدابیر:

اپنے پاسورڈ کو لمبا بنائیں،

اس طرح کے نشان ڈالیں” ‘:’;’!”^%&^%()

اپنی زبان یعنی پشتو، بلوچی، سندھی، پنجابی میں کسی بات کو لے کر پاسورڈ بنائیں، جیسے اردو کی مثال دیتا ہو کہ “$%^&@# kbjaraheho&*^%”

یعنی کوئی ایسا پاسورڈ ہو جو کوئی بھی نہ لیتا ہو، اور علاقے کا نام نہ رکھیں، کسی بندے کا نام نہ رکھیں ۔

باقی آپ کو ئی سا مشکل پاسورڈ رکھ دیں ان شاءاللہ اس حملے سے محفوظ رہینگے۔

۳۔ایکس ایس ایس ایکسپلائیٹیشن XSS/ Exploitation یا کراس سائٹ ایسکرپٹنگ /Cross-site Scripting

یہ ایک قسم کا حملہ ہے جس میں حملہ کرنے والا کسی ویب سائٹ کی کمزوری دیکھ کر اس میں اسکرپٹ /کوڈنگ کرتا ہے جس سے وہ اس ویب سائٹ دیکھنے والے لوگوں کی معلومات حاصل کرتا ہے، اور بعض اوقات کوئی پلگ اِن انسٹال کرواتا ہے، جس کی مثال میں آپ کو فیس بُک کے ہیکنگ میں بتایا تھا کہ اس ویب سائٹ کو کھولنے کے

بعد آپ کو کوئی پلگ اِن انسٹال کرنے کا بتا رہا ہوتا ہے۔ مثال کے طور پر وہ یہ دکھاتا ہے کہ اس ویڈیو کو دیکھنے کیلئے فلیش پلئیر پلگ اِن ڈالیں اور یہاں کلک کریں انسٹال کرنے کیلئے، جب آپ اس کے پلگ اِن کو انسٹال کرتے ہیں تو وہ آپ کے براوزر سے کوکیز کو چراتا ہے۔ یعنی آپ کے براوزر کے کوکیز اس حملہ کرنے والے کے پاس جائینگے، کوکیز میں آپ کے محفوظ کردہ پاسورڈ ہوتے ہیں جو آپ کسی اکاونٹ کو کھولنے کے بعد سیو پاسورڈ کرتے ہیں۔ آج کل ہیکرز اس سے بھی ایک قدم آگے گئے ہیں یعنی وہ صرف کوکیز نہیں بلکہ آپ کے ڈیٹا تک رسائی حاصل کر سکتے ہیں ۔اگر چہ فیس بک نے کافی حد تک اس حملے سے اپنے ویب سائٹ کو محفوظ بنایا ہے، مگر حملہ کرنے والا کسی دوسری جہادی ویب سائٹ کی کمزوری کو دیکھ کر یہ حملہ کر سکتا ہے، اس کی زندہ مثال عالمی اسلامی میڈیا محاذ کی ویب سائٹ پر یہ حملہ ہوا تھا یعنی gimf.com والا ویب سائٹ جس میں اسرار المجاہدین سافٹوئیر کا لنک موجود تھا، خیر بعد میں تو یہ ویب سائٹ مکمل ہیک ہوگئی تھی جب فرانس کی مبارک کاروائی ہوئی تھی ، چارلی ہیبڈو خبیثوں نے اس ویب سائٹ کو مکمل ہیک کی تھی اور نا زیبا کارٹون ڈالے تھے۔۔۔

اس سے بچنے کا طریقہ: جیسا پہلے بتا چکا ہوں کہ جب بھی آپ انٹرنیٹ استعمال کریں تو پراوئیٹ ونڈو یا انکوگنیٹو ونڈو سے استعمال کریں جس میں کوکیز اور پاسورڈ محفوظ نہیں ہوتے اور سب سے بہتر طریقہ تو یہ ہے کہ ٹور براوز ہی استعمال کریں جس میں نہ کوکیز محفوظ ہوتے ہیں اور نہ ہی کوئی اسکرپٹ اس میں کام کرتی ہے، تو جب آپ ٹور استعمال کر رہے ہوں تو کافی حد تک اس حملے سے محفوظ ہونگے۔

نوٹ: یہ آخری سبق تھا ہیکنگ کے حوالے سے جس میں بنیادی اور اپنے ڈیٹا اور اکاونٹ محفوظ بنانے سے متعلق ہیکنگ کی معلومات تھیں، باقی ویب سائٹ کی ہیکنگ اس سے علیحدہ ہے چونکہ وہ ہماری ضرورت میں نہیں اس لئے اس کے بارے میں بات نہیں ہوگی جس میں DDOS, SQL injection وغیرہ شامل ہیں۔

باقی اب آپ ہیکنگ کے عمل سے واقف ہوگئے ہیں، اب آپ خود بھی کچھ مزید احتیاط کرسکتے ہیں، مثلاً اپنے براوزر کی ہسٹری ڈیلیٹ کریں، اپنے کمپیوٹر کی ہسٹری ڈیلیٹ کریں اور بھی ایسے دیگر ہسٹری وقتاً فوقتاً ڈیلیٹ کریں، اس کے لئے ان دو سافٹوئیر کا

استعمال کریں: Auslogics Boost Speed اور Shellbag analyzer and cleaner

Auslogics کو ٹورنٹ سے ڈاونلوڈ کریں کیونکہ اس کے فری ورشن میں محدود فنکشن ہیں، اور shellbag کیلئے اس لنک پہ کلک کریں، یا انٹرنیٹ سے سرچ کر کے ڈاونلوڈ کریں۔

http://privazer.com/shellbag_analyzer_cleaner.exe